

IN THE CLAIMS

Please cancel claims 29-32, and amend the remaining claims, as follows:

1. (Currently amended) A method comprising:

forwarding peer-to-peer content between two mobile phones communicating in a cellular wireless-network via having a network infrastructure, where a mobile phone wireless-sender sends an initial message having an international mobile equipment identity, a mobile phone sender name or mobile station international integrated subscriber digital network number and encrypts protected content or content encryption key, and a mobile phone wireless-recipient consumes the protected content without requiring content personalization assistance from the network infrastructure of the cellular network.

2. (Canceled) A method according to claim 1, characterized in that the wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient.

3. (Currently amended) A method according to claim 1, wherein the mobile phone wireless-recipient sends a device certificate having a public key to the wireless sender.

4. (Currently amended) A method according to claim 3, wherein the mobile phone wireless-sender personalizes the protected content or content encryption key for the mobile phone wireless-recipient.

5. (Currently amended) A method according to claim 4, wherein the personalizing includes:

  encrypting the content or content encryption key using the public key of the mobile phone wireless-recipient;

  signing encrypted content or content encryption key using a private key of the mobile phone wireless-sender; and

  sending the protected content or content encryption key together with a device certificate of the wireless sender to the mobile phone wireless-recipient.

6. (Currently amended) A method according to claim 4, wherein the mobile phone wireless-recipient verifies forwarded protected content received from the mobile phone wireless-sender by:

  verifying the device certificate of the mobile phone wireless-sender; and  
  applying a private key of the mobile phone wireless-recipient in order for the recipient to consume the protected content.

7. (Previously presented) A method according to claim 1, wherein the protected content is digital rights management protected content.

8. (Currently amended) A cellular wireless-network comprising:

at least two mobile phoneswireless terminals;

a network infrastructure for forwarding peer-to-peer content from one mobile phonewireless terminal to another mobile phonewireless terminal;

the at least two mobile phoneswireless terminals having a peer-to-peer forwarding/reception of digital rights managementDRM-protected content module configured for either sending or receiving an initial message having an international mobile equipment identity, a mobile phone sender name or mobile station international integrated subscriber digital network number, and also configured for either encrypting or consuming protected content without content personalization assistance from the network infrastructure of the cellular network.

9. (Canceled) A wireless network according to claim 8, characterized in that the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender sends an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

10. (Currently amended) A cellular wireless-network according to claim 8, wherein the peer-to-peer forwarding/reception of digital rights managementDRM-protected content module of the mobile phonewireless recipient is configured to send a device certificate having a public key to the mobile phonewireless sender.

11. (Currently amended) A ~~cellular wireless~~-network according to claim 8, wherein the peer-to-peer forwarding/reception of ~~digital rights management~~ DRM-protected content module of the ~~mobile phone~~ wireless-sender is configured to personalize the protected content or content encryption key for the ~~mobile phone~~ wireless-recipient.

12. (Currently amended) A ~~cellular wireless~~-network according to claim 11, wherein the peer-to-peer forwarding/reception of ~~digital rights management~~ DRM-protected content module of the ~~mobile phone~~ wireless-sender is configured to personalize the content or content encryption key for the ~~mobile phone~~ wireless-recipient by:

encrypting the content or content encryption key using a public key of the ~~mobile phone~~ wireless-recipient;

signing encrypted content or content encryption key using a private key of the ~~mobile phone~~ wireless-sender; and

sending the protected content or content encryption key together with a device certificate of the ~~mobile phone~~ wireless-sender to the wireless recipient.

13. (Currently amended) A ~~cellular wireless~~-network according to claim 8,  
wherein the peer-to-peer forwarding/recipient of ~~digital rights management~~ DRM  
protected content module of the ~~mobile phone~~ wireless-recipient is configured to verify  
forwarded protected content from the ~~mobile phone~~ wireless-sender by:  
verifying a device certificate of the ~~mobile phone~~ wireless-sender; and  
applying a private key of the ~~mobile phone~~ wireless-recipient in order for the  
~~mobile phone~~ wireless-recipient to consume the protected content.

14. (Currently amended) A ~~cellular wireless~~-network according to claim 8,  
wherein the protected content is digital rights management protected content.

15. (Currently amended) A mobile phone wireless terminal comprising:  
one or more modules for operating in a cellular wireless network having another  
mobile phone wireless terminal and having a network infrastructure for forwarding peer-to-peer content from the mobile phone wireless terminal to the other mobile phone; and  
wireless terminal, each wireless terminal having  
a peer-to-peer forwarding/reception of digital rights management DRM-protected content module configured for either sending or receiving an initial message having an international mobile equipment identity, a mobile phone sender name or mobile station international integrated subscriber digital network number, and also configured for either encrypting, consuming, or a combination thereof, protected content without content personalization assistance from the network infrastructure of the cellular network.

16. (Canceled) A mobile phone wireless terminal according to claim 1,  
characterized in that the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

17. (Currently amended) A mobile phone wireless-terminal according to claim 15, wherein the peer-to-peer forwarding/reception of digital rights management DRM protected content module of the mobile phone wireless-sender is configured to personalize the protected content for the mobile phone wireless-recipient.

18. (Currently amended) A mobile phone wireless-terminal according to claim 17, wherein the peer-to-peer forwarding/reception of digital rights management DRM protected content module of the mobile phone wireless-sender is configured to personalize the content for the mobile phone wireless-recipient by:

encrypting the content or content encryption key using a public key of the mobile phone wireless-recipient;

signing encrypted content or content encryption key using a private key of the mobile phone wireless-sender; and

sending the protected content or content encryption key together with a device certificate of the mobile phone wireless-sender to the mobile phone wireless-recipient.

19. (Currently amended) A mobile phone wireless-terminal according to claim 15, wherein the peer-to-peer forwarding/reception of digital rights management DRM protected content module of the mobile phone wireless-recipient is configured to send a device certificate having a public key to the mobile phone wireless-sender.

20. (Currently amended) A mobile phone wireless terminal according to claim 15, wherein the peer-to-peer forwarding/recipient of digital rights management DRM protected content module of the mobile phone wireless-recipient is configured to verify forwarded protected content from the mobile phone wireless-sender by:

verifying a device certificate of the mobile phone wireless-sender; and

applying a private key of the mobile phone wireless-recipient in order for the mobile phone wireless-recipient to consume the protected content.

21. (Previously presented) A mobile phone wireless terminal according to claim 15, wherein the protected content is digital rights management protected content.

22. (Currently amended) A method comprising:

forwarding a protected content or content encryption key from a first mobile phone terminal to a second mobile phone in a cellular network having a network infrastructureterminal;

sending a digital rights management device certificate containing a public digital rights management key from the second mobile phone terminal to the first mobile phoneterminal;

verifying the public digital rights management key by the first mobile phoneterminal;

personalizing digital rights management content or content encryption key by encryption using a public key of the second mobile phoneterminal;

signing encrypted digital rights management content or content encryption key using a private digital rights management key of the first mobile phoneterminal;

sending encrypted and signed digital rights management content or content encryption key together with a digital rights management device certificate of the first mobile phone terminal from the first mobile phone terminal to the second mobile phoneterminal;

verifying the digital rights management device certificate of the first mobile phone terminal by the second mobile phoneterminal; and

applying a private digital rights management key of the second mobile phoneterminal, if the private digital rights management key of the first mobile phone terminal is verified, in order for the second mobile phone terminal to consume the

protected content without content personalization assistance from the network infrastructure of the cellular network.

23. (Canceled) A method according to claim 22, characterized in that the initial message includes a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof.

24. (Currently amended) A method according to claim 22, wherein the method further comprises confirming receipt of the encrypted and signed digital rights management content or content encryption key from the second mobile phone terminal to the first mobile phone terminal.

25. (Previously presented) A method according to claim 24, wherein the method further comprises sending an error message if verification of the encrypted and signed digital rights management content or content encryption key fails.

26. (Currently amended) A method according to claim 22, wherein the first mobile phone sender sends an initial message having a device certificate to the second mobile phone terminal.

27. (Currently amended) A method according to claim 1, wherein an initial message includes a device certificate to the mobile phone wireless recipient.

28. (Currently amended) Apparatus comprising:

means for forwarding peer-to-peer content between two mobile phones communicating in a cellular wireless network via having a network infrastructure; and means for sending or receiving an initial message having an international mobile equipment identity, a mobile phone sender name or mobile station international integrated subscriber digital network number, and encrypting or consuming protected content or content encryption key in a wireless sender so a wireless recipient can consume the protected content without requiring content personalization assistance from the network infrastructure of the cellular network.

29. (Canceled) Apparatus according to claim 28, wherein the apparatus further comprises:

means for sending an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient

30. (Canceled) A method according to claim 1, characterized in that the wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient.

31. (Canceled) A wireless network according to claim 8, characterized in that the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender sends an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

32. (Canceled) A wireless terminal according to claim 15, characterized in that the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

33. (Currently amended) A method according to claim 22, wherein characterized in that the initial message includes a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof.

34. (Currently amended) A method according to claim 1, wherein the mobile phone wireless-sender personalizes the protected content or content encryption key for the mobile phone wireless-recipient.